MATHEMATICS OF COMPUTATION
Volume 75, Number 255, July 2006, Pages 1519–1526
S 0025-5718(06)01827-8
Article electronically published on May 1, 2006

THE NONEXISTENCE OF NONSOLVABLE OCTIC NUMBER FIELDS RAMIFIED ONLY AT ONE SMALL PRIME

LESSENI SYLLA

Abstract. We prove that there is no primitive octic number field ramified only at one small prime, and so no such number field with a nonsolvable Galois group.

1. Introduction

At this time, there is no explicit example of a nonsolvable number field ramified at exactly one prime p, where $p < 11$. In this paper, we will show that there are no such number fields which have a nonsolvable Galois group inside S_8. We will follow the work of J. Jones [7] and S. Brueggeman [1], who found all such fields with Galois group inside S_6 and S_7, respectively. For the primes $p \geq 11$, sometimes we use the elliptic curves theory to construct a nonsolvable number field which is ramified at these desired primes. But we do not use such curves for the octic fields considered here.

In order to minimize the number of polynomials to be studied, we used, on the one hand, methods issuing from the geometry of numbers [8] and on the other, the method developed by Odlyzko, Poitou and Serre [11] for the determination of lower bounds for discriminants.

For degree 8, the minima for discriminants are only known for the totally imaginary [4] and totally real [5] signatures. We search all primitive number fields (see section 3) which are generated by the roots of an irreducible degree 8 polynomial, which are ramified at only one prime less than 11. Using discriminant bounding techniques, we eliminate number fields only ramified at 3. To eliminate 5, we use discriminant bounds depending on GRH or unconditionally by computer search. It remains to search for the two following cases: the degree 8 polynomials with a 2-power field discriminant and those with a 7-power discriminant. The result at the end shows that only the ramification at 2 is possible, and also shows that the Galois groups inside S_8 of all such fields are solvable.

This work is organized into four sections. Section 2 describes theoretical aspects of ramification. We discuss the bounds on the coefficients of the polynomials defining the number fields in section 3. In the final section, we present our results.

Received by the editor November 10, 2004 and, in revised form, May 3, 2005.
2000 *Mathematics Subject Classification.* Primary 11Y40; Secondary 11R21.
Key words and phrases. Number field, nonsolvable.

TABLE 1.

Groups	T_{37}^{+}	T_{43}	T_{48}^{+}	T_{49}^{+}	T_{50}
Orders	168	336	1344	20160	40320

2. Theory behind polynomial searches

2.1. **Galois groups of degree 8.** The notation that we use here for Galois groups of octic fields is the notation of G. Butler and J. Mckay in [2]. The nonsolvable Galois groups for the octic number fields are given in Table 1.

2.2. **Discriminant lower and upper bounds.** Diaz y Diaz established in [3] the first minima for discriminants of totally imaginary fields. The minimum for discriminants of octic number fields is 1257728. The minimum for the totally real case is 282300416 [4].

The following theorem of Ore [12] on the discriminant of a number field ramified at a prime p is essential:

Theorem 2.1. *Let K be a number field of degree n and d_K its discriminant. Let p be a prime dividing d_K and let $e_\wp$ (resp. $f_\wp$) be the ramification index (resp. the inertia degree) of a prime ideal $\wp$ lying above p. Let $n = \sum_{i=0}^{q} b_i p^i$ $(0 \leq b_i < p$ and $b_q \neq 0)$ be the p-adic representation of the integer n. Then*

i) *the maximal possible valuation of d_K in prime p is*

$$N_{n,p} = \sum_{i=0}^{q} b_i(i+1)p^i - h,$$

where h is the number of the coefficients b_i which are different from zero;

ii) *more precisely, we have*

$$v_p(d_K) \leq \sum_{\wp|p} f_\wp(e_\wp + e_\wp v_p(e_\wp) - 1). \tag{1}$$

Then $v_p(d_K)$ can assume all values from 0 to $N_{n,p}$ inclusive except $\alpha p^\alpha - 1$ if $n = p^\alpha$ or if $\alpha \geq 2$ and $n = p^\alpha + 1$.

We note that all the groups in Table 1 are primitive [6]. So in the following sections, we will look for number fields which are primitive.

Throughout the paper when the context is clear, $K = \mathbb{Q}(\theta)$ will denote an octic field, where θ is a root of an irreducible degree 8 monic polynomial and L will denote a fixed Galois closure. Its ring of integers is denoted by $\mathbb{Z}_K$ and its discriminant by d_K. The discriminant of L is denoted d_L. First we eliminate as many cases as possible by discriminant bounding arguments on either the octic field K or its Galois closure L.

2.3. **Discriminant bounding arguments.** The number field K and its Galois closure L are ramified (resp. wildly ramified) at the same single prime p.

Proposition 2.1. *If L is ramified only at 2, the possible prime ideal decompositions of the prime $p = 2$ in K are $2\mathbb{Z}_K = \wp^8$, or $2\mathbb{Z}_K = \wp_1^4\wp_2^4$ or $2\mathbb{Z}_K = \wp^4$ with inertia degree $f_\wp = 2$ in the last case. Moreover, the discriminant d_K takes its values among $\{\pm 2^{21}, \pm 2^{22}, \pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{27}, \pm 2^{28}, \pm 2^{29}, \pm 2^{30}, \pm 2^{31}\}$.*

Proof. If K is tamely ramified at 2, then by (1) we obtain $v_2(d_K) \leq 6$. Hence, $|d_K| \leq 2^6$, which is less than 1257728; this case is impossible.

So if K is ramified at 2, then it is wildly ramified. We get the prime ideal decompositions result by studying which of the different decompositions $2\mathbb{Z}_K = \prod_{\wp|2} \wp^{e_\wp}$ give the largest values of $v_2(d_K)$. The minimal absolute discriminant is greater than 2^{20}, and by Theorem 2.1 we obtain $v_2(d_K) \leq 31$. □

Proposition 2.2. *The Galois closure L of K cannot be ramified only at 3.*

Proof. If K is ramified only at 3, then by Theorem 2.1 we obtain $v_3(d_K) \leq 12$. Hence $|d_K| < 1257728$. This is a contradiction. □

Proposition 2.3. *If GRH holds, then the Galois closure L of K cannot be ramified only at 5.*

Proof. If L is tamely ramified at 5, then K is also tamely ramified at 5, and by (1) we have $v_5(d_K) \leq 7$. Hence $|d_K|$ would be less than 1257728 in this case.

Now suppose L is wildly ramified at 5 and let G be its Galois group. We show that 40 divides $|G|$, and so G is T_{50} or T_{49}^+. Let d_L be the discriminant of L and let e be the ramification index of a chosen prime ideal $\mathfrak{P}$ lying over 5 in the ring of integers of L. Using the method developed by S. Brueggeman in [1], we show that $v_5(e) = 1$. Modifying (1) of Theorem 2.1 for a Galois extension yields $v_5(d_L) \leq f(e+e-1)g \leq |G|(2-1/e)$. Hence $|d_L|^{1/|G|} \leq 5^{\frac{119}{60}} \approx 24.338$. On the other hand, the GRH implies that we have Poitou's following inequality [10]:

$$\frac{1}{|G|}\log|d_L| \geq \left(3.801 - \frac{20.766}{(\log|G|)^2} - \frac{157.914(1+1/|G|)}{(\log|G|)^3\left(1+\frac{\pi^2}{(\log|G|)^2}\right)^2}\right).$$

We obtain $|d_L|^{1/|T_{50}|} \geq 33.248$ and $|d_L|^{1/|T_{49}^+|} \geq 31.678$. This is a contradiction. □

By removing the GRH hypothesis, we get the following result:

Proposition 2.4. *If GRH does not hold, the possible ramification structures at the prime $p = 5$ in K are $5\mathbb{Z}_K = \wp_1^5\wp_2^3, 5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3, 5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3$ with inertia degree $f_{\wp_3} = 2$ or $5\mathbb{Z}_K = \wp_1^5\wp_2$ with inertia degree $f_{\wp_2} = 3$. Then the discriminant d_K takes its values among $\{5^9, 5^{10}, 5^{11}\}$.*

Proof. We get the ramification structures by studying the different decompositions $5\mathbb{Z}_K = \prod_{\wp|5} \wp^{e_\wp}$ which give the largest values of $v_5(d_K)$. By Theorem 2.1, we obtain $v_5(d_K) \leq 11$ and we use the fact that $|d_K| \geq 1257728$. Then we apply the Stickelberger identity, $d_K \equiv 0, 1 \pmod 4$. □

Proposition 2.5. *If L is ramified only at 7, the possible prime ideal decomposition of the prime $p = 7$ in K is $7\mathbb{Z}_K = \wp_1^7\wp_2$. Moreover, the discriminant d_K takes its values among $\{7^8, -7^9, 7^{10}, -7^{11}, 7^{12}, -7^{13}\}$.*

Proof. Using Theorem 2.1, we have $v_7(d_K) \leq 13$. Then we apply the Stickelberger identity and the fact that $|d_K| \geq 1257728$. □

3. Polynomials defining the octic number fields

We have shown in the previous section that the set of octic number fields K can be restricted to those which are primitive. We have also proved that the ramification at the prime $p = 3$ is not possible. Throughout this part, K will be considered primitive and p will be the prime $2, 5$ or 7.

3.1. **Notation.** Here we use the notations of [1]. Let I be the product of all prime ideals in $\mathbb{Z}_K$ above primes dividing the discriminant d_K of K. Each $\theta \in I\backslash\mathbb{Z}$ has a minimal polynomial $f_\theta(x)$ in $\mathbb{Z}[x]$ of the form

$$f_\theta(x) = x^8 + a_1x^7 + a_2x^6 + a_3x^5 + a_4x^4 + a_5x^3 + a_6x^2 + a_7x + a_8.$$

It will be sufficient to search for polynomials having a root contained in I. We need the quadratic form

$$\mathcal{T}_2 = \mathcal{T}_2(\theta) = \sum_{i=1}^{n} |\theta_i|^2$$

in the roots of f_θ, $(\theta_i)_i$, where $1 \leq i \leq 8$.

3.2. **Archimedean bounds.** We must reduce the search set of polynomials to a finite set. The coefficients a_i of f_θ are restricted by the quadratic form T_2. Hunter [7] provides a bound on T_2 which depends only on the desired discriminant and the trace. We use a version of Hunter's theorem adapted to this context by Jones and Roberts (see below). It guarantees the existence of one $\theta \in I\backslash\mathbb{Z}$ with the corresponding coefficients a_i satisfying the congruence $p^{\alpha_i}|a_i$, where α_i is a positive integer.

Theorem 3.1 (Jones and Roberts, 1999 [7])**.** *Let K be a degree $n \geq 3$, primitive number field, with discriminant d_K. Let l be the least positive integer contained in I and let m be the order of $\mathbb{Z}_K/I$. Finally, let γ_n be Hermite's constant of n-dimensional lattices. Then there exists an element $\theta \in I\backslash\mathbb{Z}$ such that*

i) $\mathcal{T}_2(\theta) \leq \frac{a_1^2}{n} + \gamma_{n-1}\left(\frac{m^2|d_K|}{l^2 n}\right)^{1/n-1}$,
ii) $0 \leq a_1 \leq nl/2$.

3.3. **Newton-Ore exponents.** Jones and Roberts define a Newton-Ore exponent, α_i, to be the largest integer such that p^{α_i} divides a_i for all polynomials f_θ with θ in the search ideal I. We search for the required minimal power of the prime p to guarantee that the polynomial discriminant is divided by a power of p. See Tables 2–7.

In the totally ramified case, we note that p divides the constant term a_8. We find the required power of p for the other a_i by using the fact that if π is a uniformizer with polynomial $F(x)$, then the different is generated by $F'(\pi)$. Details are given in [8]. For the other ramification structures, we use the method described in [7].

TABLE 2. Newton-Ore exponents for totally ramified case at 2

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
$\pm 2^{31}$	4	3	4	2	4	3	4	1
$\pm 2^{30}$	3	3	4	2	4	3	4	1
$\pm 2^{29}$	3	2	4	2	4	3	4	1
$\pm 2^{28}$	3	2	3	2	4	3	4	1
$\pm 2^{27}$	3	2	3	1	4	3	4	1
$\pm 2^{26}$	3	2	3	1	3	3	4	1
$\pm 2^{25}$	3	2	3	1	3	2	4	1
$\pm 2^{24}$	3	2	3	1	3	2	3	1
$\pm 2^{22}$	2	2	3	1	3	2	3	1
$\pm 2^{21}$	2	1	3	1	3	2	3	1

TABLE 3. Newton-Ore exponents for the other ramification structures at 2

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
$\pm 2^{22}$	3	2	3	1	4	3	4	2
$\pm 2^{21}$	2	2	3	1	3	3	4	2

TABLE 4. Newton-Ore exponents for $5\mathbb{Z}_K = \wp_1^5\wp_2^3$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
5^{11}	1	1	1	2	1	2	2	2
5^{10}	1	1	1	2	1	2	2	2
5^9	1	1	1	2	1	2	2	2

TABLE 5. Newton-Ore exponents for $5\mathbb{Z}_K = \wp_1^5\wp_2^2\wp_3$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
5^{10}	1	1	2	2	1	2	2	3
5^9	1	1	2	2	1	2	2	3

TABLE 6. Newton-Ore exponents for $5\mathbb{Z}_K = \wp_1^5\wp_2\wp_3$ or $5\mathbb{Z}_K = \wp_1^5\wp_2$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
5^9	1	2	2	2	1	2	3	4

TABLE 7. Newton-Ore exponents for $p = 7$

d_K	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
-7^{13}	1	2	2	2	2	2	1	2
7^{12}	1	2	2	2	2	2	1	2
-7^{11}	1	1	2	2	2	2	1	2
7^{10}	1	1	1	2	2	2	1	2
-7^9	1	1	1	1	2	2	1	2
7^8	1	1	1	1	1	2	1	2

Corollary 3.1. *Let K be a degree 8, primitive number field, with absolute discriminant 2^r. Then there exists an element $\theta \in I\backslash\mathbb{Z}$ such that*

1) *a) If $2\mathbb{Z}_K = \wp^8$, then $\mathcal{T}_2(\theta) \leq U_2 = \frac{a_1^2}{8} + 2^{\frac{3+r}{7}}$.*

b) If $2\mathbb{Z}_K = \wp_1^4\wp_2^4$ or $2\mathbb{Z}_K = \wp^4$, then $\mathcal{T}_2(\theta) \leq U_2 = \frac{a_1^2}{8} + 2^{\frac{5+r}{7}}$.

2) *If $d_K = \pm 2^{31}$, then $a_1 = 0$. If $d_K = \pm 2^{24}, \pm 2^{25}, \pm 2^{26}, \pm 2^{28}, \pm 2^{29}$ or $\pm 2^{30}$, then $a_1 = 0$ or $a_1 = 8$. If $d_K = \pm 2^{21}$ or $\pm 2^{22}$, then $a_1 = 0, 4$ or 8.*

When the field K is ramified only at 5, we show also that there exists an element $\theta \in I\backslash\mathbb{Z}$ such that its trace is $a_1 = 0, 5, 10, 15$ or 20.

Corollary 3.2. *Let K be a degree 8, primitive number field, with absolute discriminant 7^s. Then there exists an element $\theta \in I\backslash\mathbb{Z}$ such that*

1) $\mathcal{T}_2(\theta) \leq U_2 = \frac{a_1^2}{8} + (8 \times 7^{s+2})^{\frac{1}{7}}$,

2) $a_1 = 0, 7, 14, 21$ *or* 28.

3.4. **Coefficients bounds.** The bounds on a_1 were discussed previously. We use the method developed by M. Pohst in [10] and Newton-Ore exponents to give the values of the other coefficients a_i of the minimal polynomial f_θ.

Bounding $f_\theta(\pm 1)$, we obtain better bounds on a_5 and a_6 by using the fact that

$$a_5 = \frac{f_\theta(1) - f_\theta(-1)}{2} - (a_1 + a_3 + a_7)$$

and

$$a_6 = \frac{f_\theta(1) + f_\theta(-1)}{2} - (1 + a_2 + a_4 + a_8).$$

We can improve the results in [3] by using local corrections corresponding to small prime numbers for all signatures of octic number fields. With the results given in [11] we can eliminate many values of the constant term a_8 and discriminants d_K because of the signature.

4. Computer search results

In this section, we explain in more detail how one can make much quicker searches for primitive octic fields with 2-power, 5-power or 7-power discriminant. The program we use for these searches is written in C, using the Pari programming library [9].

Fixing the signature for the first stage, we eliminate over half of the polynomials. Then using the relation $d_{f_\theta} = d_K a^2$, where d_{f_θ} is the discriminant of f_θ, we discard all but finitely many polynomials because of the valuation at the single prime p. We check the few remaining polynomials for irreducibility: most of them are irreducible. In the final stage, we compute the field discriminants: no polynomial is found with 5-power or with 7-power field discriminant. For the polynomials with 2-power field discriminant, we determine the Galois group and a minimal polynomial which generates the same field by "polgalois" and "polredabs" commands in [9].

After eliminating duplicate fields, there are 39 distinct number fields. All of them are ramified only at 2. The search for primitive number fields of degree 8 and 5-power or 7-power discriminant came up empty in all cases. Since all of the fields found are imprimitive and so have a solvable Galois group (see Table 8), we have proved the following theorem.

Theorem 4.1. *Let K be an octic number field which is ramified at only a single prime p and $p < 11$. Then the Galois group of its Galois closure is not nonsolvable.*

TABLE 8. Search results with d_K of the form $\pm 2^r$

r	polynomials $f_\theta(x)$	signature	$Gal(L/\mathbb{Q})$
22	x^8+6x^4+1	$(0,4)$	T_4^+
24	x^8+1	$(0,4)$	T_2^+
24	$x^8+4x^6+8x^4+4x^2+1$	$(0,4)$	T_4^+
25	$x^8-4x^6+6x^4-4x^2+2$	$(0,4)$	T_{21}
26	$x^8-4x^6-2x^4-4x^2+1$	$(4,2)$	T_{10}^+
26	$x^8+4x^6-2x^4+4x^2+1$	$(0,4)$	T_{10}^+
26	$x^8+4x^4-4x^2+1$	$(0,4)$	T_{19}^+
27	x^8+2x^4+2	$(0,4)$	T_{17}
27	x^8-2x^4+2	$(0,4)$	T_{17}
27	$x^8-4x^6+10x^4-8x^2+2$	$(0,4)$	T_6
28	$x^8-4x^6-2x^4+12x^2+1$	$(4,2)$	T_{20}^+
28	$x^8+4x^6-2x^4-12x^2+1$	$(4,2)$	T_{20}^+
28	$x^8-6x^4-8x^2-1$	$(2,3)$	T_6
28	x^8-2x^4-1	$(2,3)$	T_8
28	x^8+2x^4-1	$(2,3)$	T_8
28	$x^8-4x^6+10x^4+4x^2+1$	$(0,4)$	T_{19}^+
29	$x^8-4x^6+8x^4-8x^2+2$	$(4,2)$	T_{28}
29	$x^8+4x^6+8x^4+8x^2+2$	$(0,4)$	T_{28}
29	$x^8-4x^6+4x^4-2$	$(2,3)$	T_{30}
29	$x^8+4x^6+4x^4-2$	$(2,3)$	T_{30}
30	$x^8-4x^6+2x^4+4x^2-1$	$(6,1)$	T_{27}
30	$x^8+4x^6+2x^4-4x^2-1$	$(2,3)$	T_{27}
30	$x^8-4x^6+6x^4-4x^2-1$	$(2,3)$	T_{30}
30	$x^8+4x^6+6x^4+4x^2-1$	$(2,3)$	T_{30}
30	$x^8+4x^6+2x^4+4x^2-1$	$(2,3)$	T_{30}
31	$x^8-8x^4+8x^2-2$	$(6,1)$	T_{27}
31	$x^8-8x^4-8x^2-2$	$(2,3)$	T_{27}
31	x^8-2	$(2,3)$	T_8
31	x^8+8x^4-2	$(2,3)$	T_6
31	x^8+2	$(0,4)$	T_6
31	$x^8+8x^6+20x^4+16x^2+2$	$(0,4)$	T_1
31	$x^8-8x^6+20x^4-16x^2+2$	$(8,0)$	T_1
31	x^8-4x^4+2	$(4,2)$	T_{16}
31	x^8+4x^4+2	$(0,4)$	T_{16}
31	$x^8+8x^6+24x^4+32x^2+18$	$(0,4)$	T_{17}
31	$x^8-8x^6+24x^4-32x^2+18$	$(0,4)$	T_{17}
31	$x^8+8x^6-12x^4+2$	$(4,2)$	T_7
31	$x^8-4x^4-8x^2+2$	$(4,2)$	T_{28}
31	$x^8-4x^4+8x^2+2$	$(0,4)$	T_{28}

REFERENCES

[1] S. Brueggeman. Septic Number Fields Which are Ramified Only at One Small Prime. J. Symbolic Computation 31: 549 – 555, 2001. MR1828702 (2002e:11145)

[2] G. Butler and J. Mckay. The transitive groups of degree up to eleven. Comm. Algebra 11(8) : 863 − 911, 1983. MR0695893 (84f:20005)
[3] F. Diaz y Diaz. Tables minorant la racine n-ième du discriminant d'un corps de nombres de degré n. Publications Mathématiques d'Orsay 80.06, 1980. MR0607864 (82i:12007)
[4] F. Diaz y Diaz. Petits discriminants des corps de nombres totalement imaginaires de degré 8. J. Number Theory 25: 34 − 52, 1987. MR0871167 (88a:11115)
[5] F. Diaz y Diaz, J. Martinet and M. Pohst. The minimum discriminant of totally real octic fields. J. Number Theory 36: 145 − 159, 1990. MR1072461 (91g:11128)
[6] Y. Eichenlaub. Problèmes effectifs de théorie de Galois en degré 8 à 11. Thèse soutenue à l'université de Bordeaux 1, 1996.
[7] J. Jones and D. Roberts. Sextic number fields with discriminant $(-1)^j 2^a 3^b$. In Number Theory : Fifth Conference of the Canadian Number Theory Association, CRM Proceedings and Lecture Notes 19: 141 − 172. American Mathematical Society, 1999. MR1684600 (2000b:11142)
[8] J. Martinet. Petits discriminants des corps de nombres. In Number theory days, 1980 (Exeter, 1980), volume 56 of London Math. Soc. Lecture Note Series, pages 151 − 193, Cambridge Univ. Press, Cambridge, 1982. MR0697261 (84g:12009)
[9] PARI/GP, version 2.1.5, Bordeaux, 2004, http://pari.math.u-bordeaux.fr/.
[10] M. Pohst. On the computation of number fields of small discriminants including the mininum discriminants of sixth degree fields. J. Number Theory 14: 99 − 117, 1982. MR0644904 (83g:12009)
[11] S. Selmane. Odlyzko-Poitou-Serre lower bounds for discriminants for number fields. Maghreb Math. Rev., Vol. 8, No 18.2, 1999. MR1871537 (2002j:11132)
[12] R. Thompson. On the possible forms of discriminants of algebraic fields II. American J. of Mathematics 55: 110 − 118, 1933.

Université Bordeaux 1, Laboratoire d'Algorithmique Arithmétique, 351, Cours de la Libération, 33405 Talence Cedex, France
E-mail address: Sylla.Lesseni@math.u-bordeaux1.fr